

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-152014

(43)Date of publication of application : 27.05.2004

(51)Int.Cl.

G06F 12/14

H04L 9/08

H04N 7/173

(21)Application number : 2002-316508

(71)Applicant : NIPPON HOSO KYOKAI <NHK>

(22)Date of filing : 30.10.2002

(72)Inventor : NISHIMOTO TOMONARI

BABA AKITSUGU

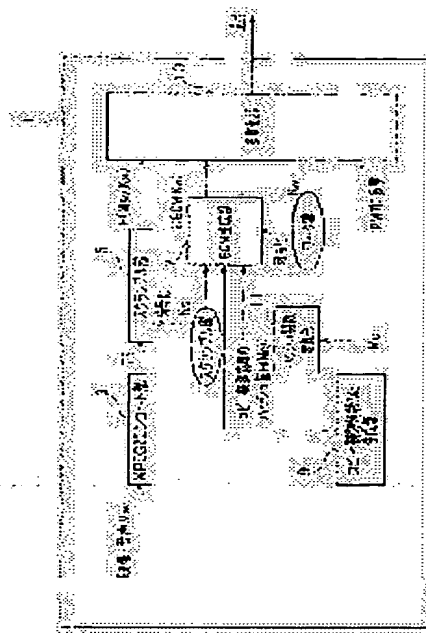
KURIOKA TATSUYA

(54) CONTENTS TRANSMITTING METHOD, CONTENTS TRANSMITTING DEVICE, CONTENTS TRANSMITTING PROGRAM, CONTENTS RECEIVING METHOD, CONTENTS RECEIVING DEVICE, AND CONTENTS RECEIVING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents transmitting method, device and program and a contents receiving method, device and program capable of preventing the illicit copying of contents.

SOLUTION: This contents transmitting device 1 transmits copy control information that is the information for controlling the copying frequency of the contents on a receiver side after receiving the contents with the contents. This device 1 has a scramble part 5 for encrypting the contents with a first encryption key to form encrypted contents, a hash function arithmetic part 11 for arithmetically operating the copy control information with a hash function and processing it to a hash value, an ECM generation part 7 for encrypting related information including the first encryption key and the function arithmetic information with a second encryption key to form first encryption key related information, and a multiplexing part 13 for multiplexing the encrypted contents, the copy control information and the first encryption key related information followed by transmitting.



LEGAL STATUS

[Date of request for examination] 10.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

THIS PAGE BLANK (USPTO)

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-152014

(P2004-152014A)

(43) 公開日 平成16年5月27日(2004.5.27)

(51) Int. Cl.⁷

G06F 12/14
H04L 9/08
H04N 7/173

F I

G06F 12/14 320E
G06F 12/14 310Z
H04N 7/173 640Z
H04L 9/00 601B

テーマコード (参考)

5B017
5C064
5J104

審査請求 未請求 請求項の数 8 O L (全 26 頁)

(21) 出願番号 特願2002-316508 (P2002-316508)
(22) 出願日 平成14年10月30日 (2002.10.30)

(71) 出願人 000004352
日本放送協会
東京都渋谷区神南2丁目2番1号
(74) 代理人 100064414
弁理士 磯野 道造
(72) 発明者 西本 友成
東京都世田谷区砧一丁目10番11号
日本放送協会 放送技術研究
所内
(72) 発明者 馬場 秋継
東京都世田谷区砧一丁目10番11号
日本放送協会 放送技術研究
所内

最終頁に続く

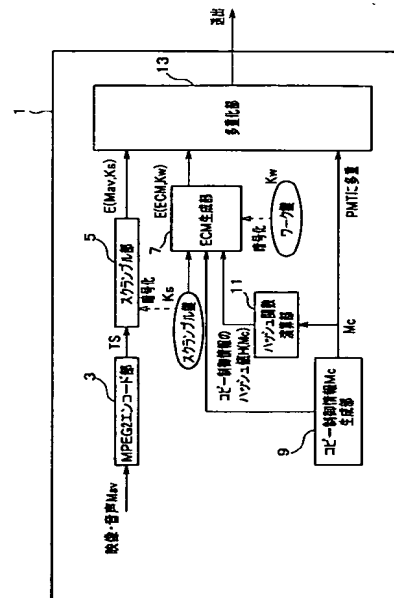
(54) 【発明の名称】 コンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラム

(57) 【要約】

【課題】コンテンツの不正コピーの防止をすることができ、コンテンツ送信、装置、プログラムおよびコンテンツ受信方法、装置、プログラムを提供する。

【解決手段】コンテンツを受信した後、この受信側において当該コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置1であって、コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするスクランブル部5と、コピー制御情報をハッシュ関数で演算し、ハッシュ値に加工するハッシュ関数演算部11と、第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とするECM生成部7と、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報を多重化して送出する多重化部13と、を備えた。

【選択図】 図1



【特許請求の範囲】

【請求項1】

コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信方法であって、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、

前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工ステップと、

前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化ステップと、

前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出ステップと、

を含むことを特徴とするコンテンツ送信方法。

【請求項2】

コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、

前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、

前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、

前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、

を備えることを特徴とするコンテンツ送信装置。

【請求項3】

コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、

前記コピー制御情報を含む前記コンテンツの利用全般に係る情報である利用条件情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、

前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、

前記暗号化コンテンツ、前記利用条件情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、

を備えることを特徴とするコンテンツ送信装置。

【請求項4】

コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信する装置を、

前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、

前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、

前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、

前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、

として機能させることを特徴とするコンテンツ送信プログラム。

【請求項5】

請求項1記載のコンテンツ送信方法によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信方法であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離ステップと、

この受信分離ステップにて分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化ステップと、

前記受信分離ステップにて分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算ステップと、

前記第一暗号鍵関連情報復号化ステップにて取得された関数演算情報と、前記演算ステップにて演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較ステップと、

この関数演算情報比較ステップにおける比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御ステップと、

この第一暗号鍵送出制御ステップにおいて送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力ステップと、

を含むことを特徴とするコンテンツ受信方法。

【請求項6】

請求項2記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、

前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段と、

この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、

前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段と、

前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段と、

この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、

を備えることを特徴とするコンテンツ受信装置。

【請求項7】

請求項3記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、

前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とを分離する受信分離手段と、

この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、

10

20

30

40

50

前記受信分離手段で分離された利用条件情報を、前記送信側に備えられている所定関数と同様の所定関数で当該利用条件情報を演算し、比較用関数演算情報とする演算手段と、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段と、前記利用条件情報に基づいて、暗号化コンテンツを復号化可能か判定する判定結果を出力する利用判定手段と、
前記関数演算情報比較手段における比較結果および前記利用判定手段における判定結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、
この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、
を備えることを特徴とするコンテンツ受信装置。

【請求項 8】

請求項 4 記載のコンテンツ送信プログラムによって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にする装置を、
前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段

、
この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段、

前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段、

前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段、

この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段、

この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段、

として機能させることを特徴とするコンテンツ受信プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツ、特にデジタルコンテンツの権利管理保護の一環である不正コピーを防止して送信または受信するコンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラムに関する。

【0002】

【従来の技術】

従来、コンテンツ（特に、デジタルコンテンツ）を送受信するデジタル放送システムにおいて、当該デジタルコンテンツを受信するデジタル放送受信装置は、受信したデジタルコンテンツに含まれるPMT（Program Map Table）等にデジタルコピー制御記述子として多重化されているコピー制御情報に従って、当該受信装置に備えられている（付属している）蓄積装置（或いは、他の記憶媒体）へのデジタルコンテンツのコピー制御を行っている。

【0003】

このデジタル放送システムにおいて、特に、限定受信方式（例えば、非特許文献 1 参照）

10

20

30

40

50

の場合であっても、デジタルコンテンツ（映像、音声）はトランスポートストリームパケットにエンコード（符号化）後、暗号化（スクランブル）されるが、PMTは暗号化されておらず、デジタルコピー制御記述子（コピー制御情報）は平文（符号化または暗号化されていない情報）の状態では伝送されている。

【0004】

【非特許文献1】

電波産業会（ARIB）の標準規格「デジタル放送に使用する番組配列情報」（ARIB STD-B10）、P108、P147

【0005】

【発明が解決しようとする課題】

しかしながら、従来のデジタル放送システムにおいて、デジタルコピー制御記述子（コピー制御情報）を不正に改ざんして、例えば、デジタルコンテンツのデジタルコピー制御記述子（コピー制御情報）が「コピー禁止」となっているのを「コピー自由」にして、蓄積装置（他の記憶媒体）に蓄積することによって不正コピーされる恐れが生じるという問題がある。

・【0006】

そこで、本発明の目的は前記した従来の技術が有する課題を解消し、コンテンツの不正コピーの防止をすることができるコンテンツ送信方法、コンテンツ送信装置、コンテンツ送信プログラムおよびコンテンツ受信方法、コンテンツ受信装置、コンテンツ受信プログラムを提供することにある。

【0007】

【課題を解決するための手段】

本発明は、前記した目的を達成するため、以下に示す構成とした。

請求項1記載のコンテンツ送信方法は、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信方法であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工ステップと、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化ステップと、前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出ステップと、を含むことを特徴とする。

【0008】

この方法によれば、まず、コンテンツ暗号化ステップにおいて、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工ステップにおいて、コピー制御情報が所定関数で演算され、関数演算情報に加工される。所定関数とは、この場合、ある情報Aを当該所定関数で演算した結果、この情報Aのデータ量を縮小させると共に、解読不能にするもので、例えば、ハッシュ関数が挙げられる。そして、第一暗号鍵暗号化ステップにおいて、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出ステップにおいて、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。

【0009】

なお、第一暗号鍵を含む関連情報とは、第一暗号鍵と、コンテンツを提供した事業者ID、つまり放送局、コンテンツ制作会社等の識別情報を含む情報である。

【0010】

また、通常、受信側の限定した受信者のみが視聴できるように、送信側でコンテンツを処理することを「スクランブルする」というが、ここでは、「暗号化する」という文言で統一的に表現している。

【0011】

さらに、第一暗号鍵は、例えば、経過時間と共に数秒単位で変更されるスクランブル鍵を指すものであり、第二暗号鍵は、例えば、コンテンツの継続時間よりも長時間保持される

10

20

30

40

50

ワーク鍵を指すものである。

【0012】

請求項2記載のコンテンツ送信装置は、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、を備えることを特徴とする。

10

【0013】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工手段で、コピー制御情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵暗号化手段で、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出手段で、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。

【0014】

請求項3記載のコンテンツ送信装置は、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信するコンテンツ送信装置であって、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コピー制御情報を含む前記コンテンツの利用全般に係る情報である利用条件情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段と、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段と、前記暗号化コンテンツ、前記利用条件情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段と、を備えることを特徴とする。

20

【0015】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工手段で、コピー制御情報を含む利用条件情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵暗号化手段で、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出手段で、暗号化コンテンツ、利用条件情報および第一暗号鍵関連情報が多重化され送出される。なお、利用条件情報は、通常、汎用的なXML言語等で記述されており、コピー制御情報に比べ、データ量が格段に多いので、多重送出手段で多重化する前にDSM-CCデータカールセル等を用いた上で、暗号化コンテンツおよび第一暗号鍵関連情報に多重化される。また、DSM-CCデータカールセルは、データ放送等に使用されるダウンロードデータカールセルのことである。

30

【0016】

請求項4記載のコンテンツ送信プログラムは、コンテンツをコピーする回数を制御する情報であるコピー制御情報を当該コンテンツと共に送信する装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、前記コンテンツを第一暗号鍵で暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記コピー制御情報を所定関数で演算した関数演算情報に加工するコピー制御情報加工手段、前記第一暗号鍵を含む関連情報および前記関数演算情報を第二暗号鍵で暗号化して、第一暗号鍵関連情報とする第一暗号鍵暗号化手段、前記暗号化コンテンツ、前記コピー制御情報および前記第一暗号鍵関連情報を多重化した多重暗号化コンテンツとして送出する多重送出手段、である。

40

【0017】

かかる構成によれば、コンテンツ暗号化手段で、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報加工手段で、コピー制御情報が所定関

50

数で演算され、関数演算情報に加工される。そして、第一暗号鍵暗号化手段で、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、多重送出手段で、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。

【0018】

請求項5記載のコンテンツ受信方法は、請求項1記載のコンテンツ送信方法によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信方法であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離ステップと、この受信分離ステップにて分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化ステップと、前記受信分離ステップにて分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算ステップと、前記第一暗号鍵関連情報復号ステップにて取得された関数演算情報と、前記コピー制御情報演算ステップにて演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較ステップと、この関数演算情報比較ステップにおける比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御ステップと、この第一暗号鍵送出制御ステップにおいて送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力ステップと、を含むことを特徴とする。

【0019】

この方法によれば、まず、受信分離ステップにおいて、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化ステップにおいて、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算ステップにおいて、送信側に備えられている所定関数と同様の所定関数で、コピー制御情報が演算され、比較用関数演算情報とされる。関数演算情報比較ステップにおいて、関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵送出制御ステップにおいて、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力ステップにおいて、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

【0020】

なお、受信分離ステップにおいて、暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離されるのは、第一暗号鍵関連情報のみを、記憶されている情報が外部から読取不可能なセキュリティモジュール内で扱うためである。

【0021】

ここでは、便宜上、第一暗号鍵および第二暗号鍵で復号化されるといった表現を使用しているが、実際には、第一暗号鍵および第二暗号鍵は、例えば、スクランブル鍵、ワーク鍵等と表現されるものである。

【0022】

請求項6記載のコンテンツ受信装置は、請求項2記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段と、この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含ま

れている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段と、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているかを判定する関数演算情報比較手段と、この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、を備えることを特徴とする。

10

【0023】

かかる構成によれば、受信分離手段で、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算手段で、送信側に備えられている所定関数と同様の所定関数で、コピー制御情報が演算され、比較用関数演算情報とされる。関数演算情報比較手段で、関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵送出制御手段で、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力手段で、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

20

【0024】

請求項7記載のコンテンツ受信装置は、請求項8記載のコンテンツ送信装置によって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にするコンテンツ受信装置であって、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とを分離する受信分離手段と、この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段と、前記受信分離手段で分離された利用条件情報を、前記送信側に備えられている所定関数と同様の所定関数で当該利用条件情報を演算し、比較用関数演算情報とする演算手段と、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているかを判定する関数演算情報比較手段と、前記利用条件情報に基づいて、暗号化コンテンツを復号化可能か判定し、判定した判定結果を出力する利用判定手段と、前記関数演算情報比較手段における比較結果および前記利用判定手段における判定結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段と、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段と、を備えることを特徴とする。

30

【0025】

かかる構成によれば、受信分離手段で、受信された多重暗号化コンテンツが暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算手段で、送信側に備えられている所定関数と同様の所定関数で、利用条件情報が演算され、比較用関数演算情報とされる。関数演算情報比較手段で、関数演算情報と比較用関数演算情報とが比較され、利用判定手段で、暗号化コンテンツが復号化可能か判定され、これら比較結果、判定結果に基づき、第一暗号鍵送出制御手段で、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力手段で、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

40

【0026】

50

なお、利用条件情報は、受信後、蓄積装置等に蓄積させた場合のコンテンツの視聴有効期間や、再生可能回数、再生可能時間、早送り再生等の特殊再生の可否（CMとはし等）、ノンリニア再生の可否等の、受信側でコンテンツを利用する際の条件となる詳細な制御情報のことである。また、所定関数の演算は、外部から記憶されている情報が読取不可能なセキュリティモジュール等の内部で行われる。

【0027】

請求項8記載のコンテンツ受信プログラムは、請求項4記載のコンテンツ送信プログラムによって送信された多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されているコピー制御情報が改ざんされていない場合に、当該コンテンツを利用可能にする装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、前記多重暗号化コンテンツを受信して、当該多重暗号化コンテンツに多重化されている暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とを分離する受信分離手段、この受信分離手段で分離された第一暗号鍵関連情報を、送信側に備えられている第二暗号鍵と同様の第二暗号鍵で復号化し、第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報を取得する第一暗号鍵関連情報復号化手段、前記受信分離手段で分離された暗号化コンテンツおよびコピー制御情報からコピー制御情報を抽出し、前記送信側に備えられている所定関数と同様の所定関数で当該コピー制御情報を演算し、比較用関数演算情報とする演算手段、前記第一暗号鍵関連情報復号化手段で取得された関数演算情報と、前記演算手段で演算された比較用関数演算情報とを比較し、前記関数演算情報に加工する前の原文データであるコピー制御情報が改ざんされているか否かを判定する関数演算情報比較手段、この関数演算情報比較手段における比較結果に基づいて、前記第一暗号鍵の送出を制御する第一暗号鍵送出制御手段、この第一暗号鍵送出制御手段で送出された第一暗号鍵で、前記暗号化コンテンツを復号化して出力するコンテンツ復号化出力手段、である。

【0028】

かかる構成によれば、受信分離手段で、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報復号化手段で、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。演算手段で、コピー制御情報が送信側に備えられている所定関数と同様の所定関数で演算され、比較用関数演算情報とされる。関数演算情報比較手段で、関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵送出制御手段で、第一暗号鍵の送出が制御される。その後、コンテンツ復号化出力手段で、暗号化コンテンツが第一暗号鍵で復号化されて出力される。

【0029】

【発明の実施の形態】

以下、本発明の一実施の形態について、図面を参照して詳細に説明する。

（コンテンツ送信装置の構成：第一の実施形態）

図1に示すコンテンツ送信装置のブロック図を参照して、コンテンツ送信装置（第一の実施の形態）の構成について説明する。図1に示すように、コンテンツ送信装置1は、MP E G 2エンコード部3と、スクランブル部5と、ECM生成部7と、コピー制御情報MC生成部9と、ハッシュ関数演算部11と、多重化部13とを備えている。

【0030】

コンテンツ送信装置1は、コンテンツ（デジタルコンテンツ、以下、コンテンツに統一して表記する）を受信した受信側で、利用する（再生する）際にコピー（複製）の制御を可能にして当該コンテンツを送信するものである。

【0031】

MP E G 2エンコード部3は、入力された映像音声コンテンツである映像音声M a v（コンテンツ）を符号化（エンコード）して、MP E G 2形式の映像音声コンテンツストリーム（T S）を生成するものである。なお、エンコードとは、映像音声信号からデジタル符

10

20

30

40

50

号を生成することであり、エンコードの目的は、アナログ信号をデジタル信号に変換することや、デジタル信号の冗長度を減らすことで、元の信号を圧縮して伝送または蓄積されるデータ量を減少させること等が挙げられる。

【0082】

スクランブル部5は、MPEG2エンコード部3でエンコードされた映像音声コンテンツストリーム(TS)をスクランブル鍵KSでスクランブルして、暗号化コンテンツ(E(MaV, KS))を生成するものである。このコンテンツ送信装置1には、スクランブル鍵KSを生成するスクランブル鍵生成手段(図示せず)が備えられている。スクランブルは、ストリーム形式の信号の暗号化を指すものであり、スクランブル鍵KSは、コンテンツの経過時間に伴い、数秒単位(一般的には1秒程度)で変更される暗号鍵である。なお、このスクランブル部5が特許請求の範囲の請求項に記載したコンテンツ暗号化手段に相当するものであり、スクランブル鍵KSが第一暗号鍵に相当するものである。

10

【0083】

ECM生成部7は、スクランブル鍵KSを含む関連情報と、ハッシュ関数演算部11で演算されたハッシュ値H(Mc)とをワーク鍵Kwで暗号化して、受信側で映像音声MaVを再生する時に用いられる第一暗号鍵関連情報(E(ECM, Kw))を生成するものである。スクランブル鍵KSを含む関連情報とは、スクランブル鍵KSと、コンテンツを提供した事業者ID、つまり放送局、コンテンツ制作会社等の識別情報を含む情報のことである。ハッシュ値H(Mc)は、原文データ(元々の情報、原文、或いは、平文ともいう)をハッシュ関数(後記する)で演算した生成データであり、この生成データから原文データを推定することが不可能なものである。ハッシュ値H(Mc)が特許請求の範囲の請求項に記載した関数演算情報に相当するものである。

20

【0084】

第一暗号鍵関連情報は、いわゆるECM(Entitlement Control Message: 共通情報)であり、この第一暗号鍵関連情報(E(ECM, Kw))は、受信側のコンテンツ受信装置(後記する)で暗号化コンテンツを復号化する際に用いられるものである。ワーク鍵Kwは、送信側であるコンテンツ送信装置1と受信側であるコンテンツ受信装置(後記する)との間で、長期間にわたり共通に保持される暗号鍵である。ECMは、コンテンツに関する情報やデスクランブルを行うための鍵情報等から構成され、暗号化された暗号箇所と暗号化されていない非暗号箇所とを含んでなるものである。なお、ワーク鍵Kwが特許請求の範囲の請求項に記載した第二暗号鍵に相当するものである。

30

【0085】

コピー制御情報Mc生成部9は、コンテンツ送信者側(放送局側、コンテンツ制作者側)の意図に応じたコピー制御情報Mcを生成するものであり、このコピー制御情報Mcは、例えば、「コピー禁止」、「コピー世代可(コピー1回可能)」、「コピー自由」といったように、受信側にてコンテンツのコピー(複製)を制御するための情報である。なお、このコピー制御情報Mcは数十バイトのバイナリの情報である。

【0086】

ハッシュ関数演算部11は、コピー制御情報Mc生成部9で生成されたコピー制御情報Mcをハッシュ関数で演算し、ハッシュ値H(Mc)を生成し、ECM生成部7に出力するものである。ハッシュ関数は、任意の長さの原文データを固定長の生成データに圧縮するための関数であって、例えば、SHA-1や、MD5というハッシュ関数が代表的なもので、これらSHA-1およびMD5は、双方とも一方向関数であり、生成データから原文データの推測を不可能にするものである。なお、このハッシュ関数演算部11が特許請求の範囲の請求項に記載したコピー制御情報加工手段に相当するものであり、ハッシュ値H(Mc)が特許請求の範囲の請求項に記載した関数演算情報に相当するものである。

40

【0087】

多重化部13は、暗号化コンテンツ(E(MaV, KS))と、第一暗号鍵関連情報(E(ECM, Kw))と、コピー制御情報とを多重化した多重暗号化コンテンツをMPEG

50

2トランスポートストリーム形式で送出するものである。また、この多重化部13は、図示を省略したデータ放送コンテンツも多重暗号化コンテンツに多重して、送出することができる。なお、コピー制御情報Mcは、映像音声コンテンツストリーム(TS)のPMT(Ptrоgram Map Table)に多重化されている。また、この多重化部13が特許請求の範囲の請求項に記載した多重送出手段に相当するものである。

【0038】

このコンテンツ送信装置1によれば、スクランブル部5で、映像音声コンテンツストリーム(TS)がスクランブル鍵KSでスクランブルされ、暗号化コンテンツ(E(MaV, KS))とされる。また、コピー制御情報Mc生成部9で生成されたコピー制御情報Mcがハッシュ関数演算部11で演算され、ハッシュ値H(Mc)が生成される。そして、ECCM生成部7で、スクランブル鍵KSを含む関連情報と、コピー制御情報Mcのハッシュ値H(Mc)とがワーク鍵Kwで暗号化され、第一暗号鍵関連情報(E(ECCM, Kw))とされる。その後、多重化部13で、暗号化コンテンツ(E(MaV, KS))と、第一暗号鍵関連情報(E(ECCM, Kw))と、コピー制御情報Mcとが多重化されて多重暗号化コンテンツとして出力される。

10

【0039】

このため、受信側にて、多重暗号化コンテンツに多重化されているハッシュ値H(Mc)と、受信側で送信側のハッシュ関数演算部11に備えられるハッシュ関数と同様のハッシュ関数でコピー制御情報Mcが演算されて得られたハッシュ値H(Mc)とが比較されれば、この比較結果に基づいて、映像音声MaV(コンテンツ)が利用可能かどうかを判定することができる。

20

【0040】

つまり、比較結果により、多重化されていたハッシュ値H(Mc)と受信側で演算したハッシュ値H(Mc)とが一致した場合、コピー制御情報Mcが改ざんされていないことになり、映像音声MaV(コンテンツ)の利用が許可される。また、多重化されていたハッシュ値H(Mc)と受信側で演算したハッシュ値H(Mc)とが一致しない場合、コピー制御情報Mcが改ざんされたことになり、映像音声MaV(コンテンツ)の利用が不許可とされる。

【0041】

これにより、映像音声MaV(コンテンツ)の不正コピーの防止、または、不正なコピー制御情報を含む映像音声MaV(コンテンツ)の生成を防止することができる。

30

【0042】

(コンテンツ受信装置の構成：第一の実施の形態)

次に、図2に示すコンテンツ受信装置のブロック図を参照して、コンテンツ受信装置(第一の実施の形態)の構成について説明する。この図2に示すように、コンテンツ受信装置21は、受信分離部23と、コピー制御情報Mc抽出部25と、ハッシュ関数演算部27と、セキュリティモジュール29と、デスクランブル部37と、MPEG2デコード部39と、コンテンツ蓄積部41とを備えている。

【0043】

コンテンツ受信装置21は、送信側のコンテンツ送信装置1(図1参照)から送信された多重暗号化コンテンツを受信し、この多重暗号化コンテンツに多重化されているコピー制御情報Mcを送信側のコンテンツ送信装置1に備えられているハッシュ関数で演算して、当該多重暗号化コンテンツに多重化されているハッシュ値H(Mc)と比較することと、コピー制御情報Mcが改ざんされていないことを検出し、これに基づいて、暗号化コンテンツ(E(MaV, KS))をデスクランブルして利用するものである。例えば、このコンテンツ受信装置21でデスクランブルされた映像音声MaVをディスプレイ(TV等)に出力したり、多重化されているコピー制御情報Mcに基づいて、当該映像音声MaVを蓄積したりすることができる。

40

【0044】

受信分離部23は、送信側のコンテンツ送信装置1から送信された多重暗号化コンテンツ

50

を受信して、暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mcと、第一暗号鍵関連情報(E(ECM, Kw))とを分離し、暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mcをコピー制御情報Mc抽出部25に出力すると共に、第一暗号鍵関連情報(E(ECM, Kw))をセキュリティモジュール29に出力するのである。つまり、この受信分離部23では、受信したMP EG2トランスポートストリームのパケット(多重暗号化コンテンツ)をフィルタリングして、映像音声パケット(暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mc)と、ECMパケット(第一暗号鍵関連情報(E(ECM, Kw)))とに分離する。なお、この受信分離部23が特許請求の範囲の請求項に記載した受信分離手段に相当するものである。

【0045】

コピー制御情報Mc抽出部25は、受信分離部23で分離された暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mcから、コピー制御情報Mcを抽出して、ハッシュ関数演算部27と外部の蓄積装置(図示せず)に出力すると共に、暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mcをデスクランブル部37に出力するのである。つまり、このコピー制御情報Mc抽出部25は、コピー制御情報Mcを外部に出力することにより、外部の蓄積装置等で映像音声MaVを再暗号化してから、当該コピー制御情報Mcに基づいて再暗号化した映像音声MaVを取り扱えるようにしている。

【0046】

また、コピー制御情報Mcは、暗号化コンテンツ(E(MaV, KS))のPMT部に記憶されている(含まれている)ので、分離させずにデスクランブル部37に出力される。また、外部の蓄積装置(図示せず)は、例えば、D-VHS等であり、コピー制御情報Mc抽出部25で抽出されたコピー制御情報Mcは、IEEE1394等のホームネットワークを介して、当該蓄積装置に出力される。

【0047】

なお、このコピー制御情報Mc抽出部25でコピー制御情報Mcが抽出され、不正に改ざんされた場合、セキュリティモジュール29内の送出制御部35でスクランブル鍵KSの送出が停止されるため、スクランブルされている暗号化コンテンツ(E(MaV, KS))をデスクランブルできない。つまり、不正に改ざんされたコピー制御情報Mcに基づいてコンテンツ蓄積部41に、暗号化コンテンツ(E(MaV, KS))がスクランブルされたまま蓄積されることになって、映像音声MaV(コンテンツ)を不正利用することができない。

【0048】

また、IEEE1394等のホームネットワークを介して、外部の蓄積装置(図示せず)にコピー制御情報Mcを蓄積する場合も同様に、不正に改ざんされたコピー制御情報Mcに基づいて、IEEE1394の伝送保護技術であるDTPで暗号化コンテンツ(E(MaV, KS))が伝送される(送出される)がスクランブルされたままDTPで保護されるため、映像音声MaV(コンテンツ)を不正利用することができない。補足しておくとして、この実施の形態では、多重暗号化コンテンツのPMTの部分に、コピー制御情報Mcを暗号化せずに平文のまま、多重して送信する既存の送出方法で送出しているため、既存のコンテンツ受信装置に悪影響を及ぼすことはない。

【0049】

ハッシュ関数演算部27は、コピー制御情報Mc抽出部25で抽出されたコピー制御情報Mcをハッシュ関数で演算し、ハッシュ値H(Mc)を生成してセキュリティモジュール29に出力するのである。このハッシュ関数演算部27で使用されるハッシュ関数は、送信側のコンテンツ送信装置1のハッシュ関数演算部11に備えられるハッシュ関数と同一のものであり、このハッシュ関数演算部27で演算されたハッシュ値H(Mc)が特許請求の範囲の請求項に記載した比較用関数演算情報に相当するものである。このハッシュ関数演算部27で演算されたハッシュ値H(Mc)を以下、比較用ハッシュ値H(Mc)と記載することにする。このハッシュ関数演算部27が特許請求の範囲の請求項に記載した演算手段に相当するものである。

10

20

30

40

50

【0050】

セキュリティモジュール29は、ICカード等によって構成され、内部に記録した情報が外部より読取不可能に構成されており、耐タンパー性（耐衝撃性）を備えたモジュールであり、ECM解析部31と、比較部33と、送出制御部35とを備えている。

【0051】

ECM解析部31は、第一暗号鍵関連情報（E（ECM，Kw））を、予め送信側のコンテンツ送信装置1と受信側のコンテンツ受信装置21とで共通に保持されているワーク鍵Kwで復号化して、スクランブル鍵KSと、コピー制御情報Mcのハッシュ値H（Mc）とを取得し、スクランブル鍵KSを送出制御部35に出力すると共に、ハッシュ値H（Mc）を比較部33に出力するものである。このECM解析部31が特許請求の範囲の請求項に記載した第一暗号鍵関連情報復号化手段に相当するものである。

10

【0052】

比較部33は、ECM解析部31で取得されたハッシュ値H（Mc）と、ハッシュ関数演算部27で演算された比較用ハッシュ値H（Mc）とを比較して、一致していた場合、送出制御部35にスクランブル鍵KS送出許可信号を出力すると共に、一致していない場合、送出制御部35にスクランブル鍵KS送出不可信号を出力するものである。スクランブル鍵KS送出許可信号は、送出制御部35からセキュリティモジュール29の外部にスクランブル鍵KSの出力を許可する信号で、スクランブル鍵KS送出不可信号は、送出制御部35からセキュリティモジュール29の外部にスクランブル鍵KSの出力を不可にする信号である。

20

【0053】

なお、この比較部33が特許請求の範囲の請求項に記載した関数演算情報比較手段に相当するものであり、これらスクランブル鍵KS送出許可信号およびスクランブル鍵KS送出不可信号が特許請求の範囲の請求項に記載した比較結果に相当するものである。

【0054】

送出制御部35は、比較部33から出力されたスクランブル鍵KS送出許可信号またはスクランブル鍵KS送出不可信号に基づいて、ECM解析部31から入力されたスクランブル鍵KSの出力を制御するものである。この送出制御部35が特許請求の範囲の請求項に記載した第一暗号鍵送出制御手段に相当するものである。

【0055】

デスクランブル部37は、暗号化コンテンツ（E（MaV，KS））をセキュリティモジュール29の送出制御部35から出力されたスクランブル鍵KSでデスクランブルして、MP EG2形式の映像音声コンテンツストリーム（TS）を生成するものである。

30

【0056】

MP EG2デコード部39は、デスクランブル部37から出力されたMP EG2形式の映像音声コンテンツストリーム（TS）をデコードした映像音声MaVをコンテンツ受信装置21の外部に備えられる表示装置（図示せず）に送出するものである。なお、デスクランブル部37およびMP EG2デコード部39が特許請求の範囲の請求項に記載したコンテンツ復号化出力手段に相当するものである。

【0057】

コンテンツ蓄積部41は、大容量のハードディスク等によって構成され、コピー制御情報Mc抽出部25から出力された暗号化コンテンツ（E（MaV，KS））を蓄積すると共に、デスクランブル部37でデスクランブルされた映像音声MaV（コンテンツ）を蓄積するものである。但し、コピー制御情報Mc抽出部25で抽出されたコピー制御情報Mcが「コピー禁止」であれば、デスクランブルされた映像音声MaV（コンテンツ）を蓄積することができず、この旨を通知するメッセージ（「コピー禁止のコンテンツであるので蓄積できません！」等のメッセージ）が図示を省略した表示部に表示される。

40

【0058】

このコンテンツ受信装置21によれば、受信分離部23で、受信された多重暗号化コンテンツが暗号化コンテンツ（E（MaV，KS））およびコピー制御情報Mcと、第一暗号

50

鍵関連情報 (E (ECM, Kw)) とに分離される。続いて、ECM解析部 31 で、第一暗号鍵関連情報 (E (ECM, Kw)) がワーク鍵 Kw で復号化され、この第一暗号鍵関連情報 (E (ECM, Kw)) に含まれているスクランブル鍵 Ks およびハッシュ値 H (Mc) が取得される。ハッシュ関数演算部 27 で、送信側のコンテンツ送信装置 1 に備えられているハッシュ関数と同様のハッシュ関数で、コピー制御情報 Mc が演算され、比較用ハッシュ値 H (Mc) とされる。比較部 33 で、ハッシュ値 H (Mc) と比較用ハッシュ値 H (Mc) とが比較され、この比較結果に基づき、送出制御部 35 で、スクランブル鍵 Ks の送出が制御される。その後、デスクランブル部 37 で、暗号化コンテンツ (E (MaV, Ks)) がスクランブル鍵 Ks で復号化され、MP EG 2 デコード部 39 でデコードされ、映像音声 MaV (コンテンツ) として出力される。

10

【0059】

このため、多重暗号化コンテンツに多重化されているハッシュ値 H (Mc) と、送信側のハッシュ関数演算部 11 に備えられるハッシュ関数と同様のハッシュ関数でコピー制御情報 Mc が演算されて得られた比較用ハッシュ値 H (Mc) とが比較され、この比較結果に基づいて、映像音声 MaV (コンテンツ) が利用可能かどうかを判定することができる。

【0060】

つまり、比較結果により、多重化されていたハッシュ値 H (Mc) と演算して得られた比較用ハッシュ値 H (Mc) とが一致した場合、コピー制御情報 Mc が改ざんされていないことになり、映像音声 MaV (コンテンツ) の利用が許可される。また、多重化されていたハッシュ値 H (Mc) と受信側で演算したハッシュ値 H (Mc) とが一致しない場合、コピー制御情報 Mc が改ざんされたことになり、映像音声 MaV (コンテンツ) の利用が不許可とされる。これにより、映像音声 MaV (コンテンツ) の不正コピーの防止、または、不正なコピー制御情報を含む映像音声 MaV (コンテンツ) の生成を防止することができる。

20

【0061】

なお、このコンテンツ受信装置 21 では、ハッシュ関数演算部 27 でコピー制御情報 Mc をハッシュ関数で演算して、比較用ハッシュ値 H (Mc) を生成して、比較部 33 でハッシュ値 H (Mc) と比較用ハッシュ値 H (Mc) とを比較したが、予め、送信側のコンテンツ送信装置 1 において、第一暗号鍵関連情報 (E ECM, Kw) にハッシュ値 H (Mc) を含めるのではなくコピー制御情報 Mc を含めておき、セキュリティモジュール 29 内の比較部 33 で、コピー制御情報 Mc 同士を比較してもよい。

30

【0062】

ただし、コピー制御情報 Mc は、映像、音声、データなどのコンポーネント毎に付与することができ、数十バイトに膨れ上がる可能性があるため、送信側のコンテンツ送信装置 1 において、ハッシュ関数で演算してハッシュ値 H (Mc) を生成した方が、ECM生成部 7 で E (ECM, Kw) のデータ量を小さく生成することができ、放送伝送帯域を効率的に利用することができる。また、この実施の形態では、ハッシュ関数演算部 27 をセキュリティモジュール 29 の外部に設けたが、このハッシュ関数演算部 27 をセキュリティモジュール 29 の内部に設けてもよい。

40

【0063】

(コンテンツ送信装置の動作：第一の実施の形態)

次に、図 3 に示すフローチャートを参照して、コンテンツ送信装置の動作を説明する (適宜図 1 参照)。

まず、コンテンツ送信装置 1 の MP EG 2 エンコード部 3 に映像音声 MaV (コンテンツ) が入力され、この MP EG 2 エンコード部 3 で映像音声 MaV (コンテンツ) がエンコードされて、MP EG 2 形式の映像音声コンテンツストリーム (TS) とされスクランブル部 5 へ出力される (S1)。

【0064】

続いて、スクランブル部 5 で映像音声コンテンツストリーム (TS) がスクランブル鍵 Ks でスクランブルされて、暗号化コンテンツ (E (MaV, Ks)) とされ、多重化部 1

50

3へ出力される(S2)。このスクランブル部5で使用されたスクランブル鍵KSに当該スクランブル鍵KSに関する情報が付加されて、スクランブル鍵KSを含む関連情報とされ、このスクランブル鍵KSを含む関連情報がECM生成部7に入力される。

【0065】

また、コピー制御情報Mc生成部9でコピー制御情報Mcが生成され、ハッシュ関数演算部11と多重化部13へ出力される(S3)。なお、コピー制御情報Mcは、多重化部13においてPMTに多重化される。すると、ハッシュ関数演算部11でコピー制御情報Mcが当該ハッシュ関数演算部11に備えられているハッシュ関数によって演算され、ハッシュ値H(Mc)とされてECM生成部7へ出力される(S4)。

【0066】

そして、ECM生成部7で、スクランブル鍵KSを含む関連情報とハッシュ値H(Mc)とがワーク鍵Kwで暗号化され、第一暗号鍵関連情報(E(ECM, Kw))とされて多重化部13に出力される(S5)。その後、多重化部13で暗号化コンテンツ(E(MaV, KS))、第一暗号鍵関連情報(E(ECM, Kw))およびコピー制御情報Mc(PMTとして)が多重化され、多重暗号化コンテンツとされて、送出される(S6)。

【0067】

(コンテンツ受信装置の動作：第一の実施の形態)

次に、図4、図5に示すフローチャートを参照して、コンテンツ受信装置21の動作を説明する(適宜図2参照)。なお、このコンテンツ受信装置21の動作の説明では、送信側のコンテンツ送信装置1から送信された多重暗号化コンテンツを受信した後、コピー制御情報Mcが改ざんされているか否かにより、映像音声MaV(コンテンツ)を再生するまでの概略を説明したものである。また、このコンテンツ受信装置21の動作の説明では、多重暗号化コンテンツを復号化またはデスクランブルにかかるとの情報のみに言及して説明している。

【0068】

送信側のコンテンツ送信装置1から送出された多重暗号化コンテンツが、コンテンツ受信装置21の受信分離部23で受信される(S11)。すると、受信分離部23で多重暗号化コンテンツが分離され、暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mcがコピー制御情報Mc抽出部25へ出力されると共に、第一暗号鍵関連情報(E(ECM, Kw))がECM解析部31へ出力される(S12)。

【0069】

そして、コピー制御情報Mc抽出部25でコピー制御情報Mcが抽出され、ハッシュ関数演算部27と外部の蓄積装置(図示せず)等へ出力されると共に、暗号化コンテンツ(E(MaV, KS))およびコピー制御情報Mcがデスクランブル部37へ出力される(S13)。すると、ハッシュ関数演算部27でコピー制御情報Mcがハッシュ関数で演算され、比較用ハッシュ値H(Mc)が生成され、比較部33へ出力される(S14)。また、ECM解析部31で第一暗号鍵関連情報(E(ECM, Kw))がワーク鍵Kwで復号化され、ハッシュ値H(Mc)およびスクランブル鍵KSが取得され、ハッシュ値H(Mc)が比較部33へ出力されると共に、スクランブル鍵KSが送出制御部35へ出力される(S15)。これより図5を参照する。

【0070】

そして、比較部33でハッシュ値H(Mc)と比較用ハッシュ値H(Mc)とが比較され、一致するかが判定される(S16)。つまり、このS16にて、比較部33でハッシュ値H(Mc)と比較用ハッシュ値H(Mc)とが比較された結果(比較結果)によって、コピー制御情報Mcが改ざんされたかが判断できる。すなわち、比較結果が一致していれば、改ざんされていないと判断でき、一致していなければ、改ざんされていると判断できる。

【0071】

この比較部33でハッシュ値H(Mc)と比較用ハッシュ値H(Mc)とが一致すると判定された場合(S16、YES)、比較部33からスクランブル鍵KS送出許可信号(図

10

20

30

40

50

中、許可信号)が送出制御部35へ出力される(S17)。送出制御部35で、スクランブル鍵KS送出許可信号に基づいて、スクランブル鍵KSがデスクランブル部37へ出力される(S18)。デスクランブル部37で暗号化コンテンツ(E(MaV, KS))がデスクランブルされ、MPEG2形式の映像音声コンテンツストリーム(TS)が得られ、MPEG2デコード部39に出力される(S19)。MPEG2デコード部39で、MPEG2形式の映像音声コンテンツストリーム(TS)がデコードされ映像音声MaV(コンテンツ)が出力される(S20)。

【0072】

また、S16にて、ハッシュ値H(Mc)と比較用ハッシュ値H(Mc)とが一致しないと判定された場合(S16、NO)、比較部38からスクランブル鍵KS送出不可信号(図中、不可信号)が送出制御部35へ出力され(S21)、暗号化コンテンツ(E(MaV, KS))を再生できない旨のメッセージが図示を省力した表示部に表示される(S22)。

【0073】

(コンテンツ送信装置の構成：第二の実施形態)

図6は、図1に示したコンテンツ送信装置1の別の実施の形態(第二の実施の形態)であるコンテンツ送信装置1Aのブロック図であり、この図6を参照して、コンテンツ送信装置1Aの構成を説明する。なお、コンテンツ送信装置1の構成と同一の構成は、同一の符号を付してその説明を省略する。

【0074】

図6に示したこのコンテンツ送信装置1Aはマークアップ記述言語型利用条件情報MmI生成部51を備えており、このマークアップ記述言語型利用条件情報MmI生成部51は、XML(eXtensible Markup Language)等のマークアップ記述言語で記述された、コンテンツの利用条件を規定した利用条件情報MmIを生成するものである。この利用条件情報MmIは、コピー制御情報Mcを含んでおり、その他にも受信側で蓄積した映像音声MaV(コンテンツ)の視聴有効期間や、再生可能回数、再生可能時間、早送り再生等の特殊再生の可否、ノンリニア再生(不連続再生)の可否等の映像音声MaV(コンテンツ)の利用に関する詳細な制御情報である。

【0075】

XMLは汎用的なコンピュータ言語(マークアップ記述言語)であり、様々な端末機器(例えば、後記するコンテンツ受信装置21A)で利用することができ。また、映像音声MaV(コンテンツ)の利用条件情報MmIにマークアップ記述言語を用いると、バイナリで記述するよりもデータサイズ(データ量)が大きくなるため、コピー制御情報Mc単独の場合とは異なり、PMT等に多重化することが困難である。このため、この実施の形態では、利用条件情報MmIはDSM-CCデータカルセル(Digital Stream Command and Control:ダウンロードカルセル方式)等を用いて多重化する。

【0076】

このコンテンツ送信装置1Aによれば、スクランブル部5で、映像音声コンテンツストリーム(TS)がスクランブル鍵KSでスクランブルされ、暗号化コンテンツ(E(MaV, KS))とされる。また、マークアップ記述言語型利用条件情報MmI生成部51で生成された利用条件情報MmIがハッシュ関数演算部11で演算され、ハッシュ値H(MmI)が生成される。そして、ECM生成部7で、スクランブル鍵KSを含む関連情報と、利用条件情報MmIのハッシュ値H(MmI)とがワーク鍵Kwで暗号化され、第一暗号鍵関連情報(E(ECM, Kw))とされる。その後、多重化部13で、暗号化コンテンツ(E(MaV, KS))と、第一暗号鍵関連情報(E(ECM, Kw))と、利用条件情報MmIとが多重化されて多重暗号化コンテンツとして出力される。

【0077】

このため、受信側にて、多重暗号化コンテンツに多重化されているハッシュ値H(MmI)と、受信側で送信側のハッシュ関数演算部11に備えられるハッシュ関数と同様のハッ

10

20

30

40

50

シュ関数で利用条件情報Mm1が演算されて得られたハッシュ値H(Mm1)とが比較され、さらに利用条件情報Mm1に基づいて、暗号化コンテンツ(E(MaV, KS))を復号化可能かが判定されれば、これら比較結果および判定結果に基づいて、映像音声MaV(コンテンツ)が利用可能かどうかを判定することができる。

【0078】

つまり、比較結果により、多重化されていたハッシュ値H(Mm1)と受信側で演算したハッシュ値H(Mm1)とが一致した場合、利用条件情報Mm1に含まれているコピー制御情報Mcが改ざんされていないことになり、さらに利用条件情報Mm1で示される各条件に合致していれば、映像音声MaV(コンテンツ)の利用が許可される。また、多重化されていたハッシュ値H(Mm1)と受信側で演算したハッシュ値H(Mm1)とが一致しない場合、利用条件情報Mm1に含まれているコピー制御情報Mcが改ざんされたことになり、または、利用条件情報Mm1で示される各条件に合致していなければ、映像音声MaV(コンテンツ)の利用が不許可とされる。これにより、映像音声MaV(コンテンツ)の不正コピーの防止、または、不正なコピー制御情報を含む映像音声MaV(コンテンツ)の生成を防止することができる。

【0079】

(コンテンツ受信装置の構成：第二の実施の形態)

図7は、図2に示したコンテンツ受信装置21の別の実施の形態(第二の実施の形態)であるコンテンツ受信装置21Aのブロック図であり、この図7を参照して、コンテンツ受信装置21Aの構成を説明する。なお、コンテンツ送信装置21の構成と同一の構成は、

【0080】

図7に示したコンテンツ受信装置21Aは、利用条件情報Mm1抽出部61と、セキュリティモジュール29Aに利用判定部63と備えている。利用条件情報Mm1抽出部61は、受信分離部23で分離されたDSM-CCデータカールセルから利用条件情報Mm1を抽出して、セキュリティモジュール29Aの利用判定部63および外部の蓄積装置(図示せず)に出力するものである。

【0081】

利用判定部63は、利用条件情報Mm1に含まれている各条件を判定するもので、各条件を満たしているとは判定された場合、映像音声MaV利用許可信号が送出制御部35に出力され、各条件を満たしているとは判定されない場合、映像音声MaV利用不可信号が送出制御部35に出力される。例えば、映像音声MaV(コンテンツ)の利用有効期限を過ぎていた(超過している)場合や、映像音声MaV(コンテンツ)の再生時間を過ぎていた(超過している)場合等は、映像音声MaV(コンテンツ)が利用不可能であると判定され(各条件を満たしているとは判定されない)、映像音声MaV利用不可信号が送出制御部35に出力される。

【0082】

このコンテンツ受信装置21Aによれば、受信分離部23で、受信された多重暗号化コンテンツが暗号化コンテンツ(E(MaV, KS))と、DSM-CCデータカールセル(利用条件情報Mm1)と、第一暗号鍵関連情報(E(ECM, Kw))とに分離される。続いて、ECM解析部31で、第一暗号鍵関連情報(E(ECM, Kw))がワーク鍵Kwで復号化され、この第一暗号鍵関連情報(E(ECM, Kw))に含まれているスクランブル鍵KSおよびハッシュ値H(Mm1)が取得される。ハッシュ関数演算部27で、送信側のコンテンツ送信装置1に備えられているハッシュ関数と同様のハッシュ関数で、利用条件情報Mm1が演算され、比較用ハッシュ値H(Mm1)とされる。比較部33で、ハッシュ値H(Mm1)と比較用ハッシュ値H(Mm1)とが比較される。また、利用判定部63で利用条件情報Mm1の各条件を満たしているかどうか判定される。これらの比較結果および判定結果に基づき、送出制御部35で、スクランブル鍵KSの送出が制御される。その後、デスクランブル部37で、暗号化コンテンツ(E(MaV, KS))がスクランブル鍵で復号化され、MP EG2デコード部39でデコードされ、映像音声M

αV (コンテンツ) として出力される。

【0083】

このため、多重暗号化コンテンツに多重化されているハッシュ値 $H(MmI)$ と、送信側のハッシュ関数演算部 11 に備えられるハッシュ関数と同様のハッシュ関数で利用条件情報 MmI が演算されて得られた比較用ハッシュ値 $H(MmI)$ とが比較され、この比較結果と、利用判定部 63 の判定結果とに基づいて、映像音声 $M\alpha V$ (コンテンツ) が利用可能かどうかを判定することができる。

【0084】

つまり、比較結果により、多重化されていたハッシュ値 $H(MmI)$ と演算して得られた比較用ハッシュ値 $H(MmI)$ とが一致した場合、利用条件情報 MmI が改ざんされていないことになり、映像音声 $M\alpha V$ (コンテンツ) の利用が許可される。また、多重化されていたハッシュ値 $H(MmI)$ と受信側で演算したハッシュ値 $H(MmI)$ とが一致しない場合、利用条件情報 MmI が改ざんされたことになり、映像音声 $M\alpha V$ (コンテンツ) の利用が不許可とされる。さらに、利用判定部 63 による利用条件情報 MmI の判定結果に基づき映像音声 $M\alpha V$ (コンテンツ) が利用可能かどうか判定される。

【0085】

これにより、映像音声 $M\alpha V$ (コンテンツ) の不正コピーの防止、または、不正なコピー制御情報を含む映像音声 $M\alpha V$ (コンテンツ) の生成を防止することができる。さらに、送信側の映像音声 $M\alpha V$ (コンテンツ) の制作者(放送事業者)の意図に応じて、利用条件情報 MmI を設定すること、受信側において、利用条件情報 MmI に基づいた映像音声 $M\alpha V$ (コンテンツ) の利用(再生)を実現することができる。

【0086】

(コンテンツ送信装置の動作：第二の実施の形態)

次に、図 8 に示すフローチャートを参照して、図 6 に示したコンテンツ送信装置 1A の動作を説明する。

まず、コンテンツ送信装置 1A の MPEG2 エンコード部 3 に映像音声 $M\alpha V$ (コンテンツ) が入力され、この MPEG2 エンコード部 3 で映像音声 $M\alpha V$ (コンテンツ) がエンコードされて、MPEG2 形式の映像音声コンテンツストリーム (TS) とされスクランブル部 5 へ出力される (S31)。

【0087】

続いて、スクランブル部 5 で映像音声コンテンツストリーム (TS) がスクランブル鍵 KS でスクランブルされて、暗号化コンテンツ ($E(M\alpha V, KS)$) とされ、多重化部 13 へ出力される (S32)。このスクランブル部 5 で使用されたスクランブル鍵 KS に当該スクランブル鍵 KS に関する情報が付加されて、スクランブル鍵 KS を含む関連情報とされ、このスクランブル鍵 KS を含む関連情報が ECM 生成部 7 に入力される。

【0088】

また、マークアップ記述言語型利用条件情報 MmI 生成部 51 で利用条件情報 MmI が生成され、この利用条件情報 MmI がハッシュ関数演算部 11 へ出力されると共に、多重化部 13 へ出力される (S33)。なお、利用条件情報 MmI は、コンテンツ送信装置 1A の所有者(または使用者、ユーザ)であるコンテンツ制作者、放送事業者の意図の応じて各条件が設定されて、この条件を盛り込んだものがマークアップ記述言語型利用条件情報 MmI 生成部 51 で生成される。

【0089】

すると、ハッシュ関数演算部 11 で利用条件情報 MmI が当該ハッシュ関数演算部 11 に備えられているハッシュ関数によって演算され、ハッシュ値 $H(MmI)$ とされて ECM 生成部 7 へ出力される (S34)。

【0090】

そして、ECM 生成部 7 で、スクランブル鍵 KS を含む関連情報とハッシュ値 $H(MmI)$ とがワーク鍵 Kw で暗号化され、第一暗号鍵関連情報 ($E(ECM, Kw)$) とされて多重化部 13 へ出力される (S35)。その後、多重化部 13 で暗号化コンテンツ (E (

10

20

30

40

50

Mαv、K S))、第一暗号鍵関連情報(E (ECM、K w))および利用条件情報M m lが多重化され、多重暗号化コンテンツとされて、送出される(S 36)。

【0091】

(コンテンツ受信装置の動作：第二の実施の形態)

次に、図9、図10に示すフローチャートを参照して、図7に示したコンテンツ受信装置21Aの動作を説明する。なお、このコンテンツ受信装置21Aの動作の説明では、送信側のコンテンツ送信装置1Aから送信された多重暗号化コンテンツを受信した後、利用条件情報M m lが改ざんされているか否かにより、映像音声Mαv(コンテンツ)を再生するまでの概略を説明したものである。また、このコンテンツ受信装置21Aの動作の説明では、多重暗号化コンテンツを復号化またはデスクランブルにかかると情報のみに言及して説明している。

10

【0092】

送信側のコンテンツ送信装置1Aから送出された多重暗号化コンテンツが、コンテンツ受信装置21Aの受信分離部23で受信される(S41)。すると、受信分離部23で多重暗号化コンテンツが分離され、暗号化コンテンツ(E (Mαv、K S))がデスクランブル部37へ、DSM-CCデータカプセル(利用条件情報M m l)が利用条件情報M m l抽出部61へ、第一暗号鍵関連情報(E (ECM、K w))がECM解析部31へ出力される(S42)。

【0093】

そして、利用条件情報M m l抽出部61で利用条件情報M m lが抽出され、ハッシュ関数演算部27、利用判定部63および外部の蓄積装置(図示せず)等へ出力される(S43)。すると、ハッシュ関数演算部27で利用条件情報M m lがハッシュ関数で演算され、比較用ハッシュ値H (M m l)が生成され、比較部33へ出力される(S44)。また、ECM解析部31で第一暗号鍵関連情報(E (ECM、K w))がワーク鍵K wで復号化され、ハッシュ値H (M m l)およびスクランブル鍵K Sが取得され、ハッシュ値H (M m l)が比較部33へ出力されると共に、スクランブル鍵K Sが送出制御部35へ出力される(S45)。これより図10を参照する。

20

【0094】

そして、利用判定部63で暗号化コンテンツ(E (Mαv、K S))つまり映像音声Mαvが利用可能かどうか(各条件を満たしているかどうか)が判定される(S46)。この利用判定部63で暗号化コンテンツ(E (Mαv、K S))つまり映像音声Mαvが利用可能であると判定された場合(S46、Yes)、利用判定部63から映像音声Mαv利用許可信号(図中、許可信号)が送出制御部35へ出力される(S47)。

30

【0095】

さらに、比較部33でハッシュ値H (M m l)と比較用ハッシュ値H (M m l)とが比較され、一致するか否かが判定される(S48)。つまり、このS48にて、比較部33でハッシュ値H (M m l)と比較用ハッシュ値H (M m l)とが比較された結果(比較結果)によって、利用条件情報M m lが改ざんされたか否かが判断できる。すなわち、比較結果が一致していれば、改ざんされていないと判断でき、一致していなければ、改ざんされていると判断できる。

40

【0096】

この比較部33でハッシュ値H (M m l)と比較用ハッシュ値H (M m l)とが一致すると判定された場合(S48、Yes)、比較部33からスクランブル鍵K S送出許可信号(図中、許可信号)が送出制御部35へ出力される(S49)。送出制御部35で、スクランブル鍵K S送出許可信号に基づいて、スクランブル鍵K Sがデスクランブル部37へ出力される(S50)。デスクランブル部37で暗号化コンテンツ(E (Mαv、K S))がデスクランブルされ、MP EG2形式の映像音声コンテンツストリーム(T S)が得られ、MP EG2デコード部39に出力される(S51)。MP EG2デコード部39で、MP EG2形式の映像音声コンテンツストリーム(T S)がデコードされ映像音声Mαv(コンテンツ)が出力される(S52)。

50

【0097】

また、S46にて、利用判定部63で暗号化コンテンツ(E(MaV, KS))つまり映像音声MaVが利用可能であると判定されない場合(S46、No)、利用判定部63から映像音声MaV利用不可信号(図中、不可信号)が送出制御部35へ出力される(S53)。暗号化コンテンツ(E(MaV, KS))つまり映像音声MaVを再生できない旨(利用条件情報MmIによる)のメッセージが図示を省力した表示部に表示される(S54)。

【0098】

また、S48にて、比較部33でハッシュ値H(MmI)と比較用ハッシュ値H(MmI)とが一致しないと判定された場合(S48、No)、比較部33からスクランブル鍵KS送出不可信号(図中、不可信号)が送出制御部35へ出力され(S55)、暗号化コンテンツ(E(MaV, KS))つまり映像音声MaVを再生できない旨のメッセージが図示を省力した表示部に表示される(S56)。

【0099】

(デジタルコピー制御記述子について)

最後に、デジタル制御記述子について説明する。図11は、デジタルコピー制御記述子(データテーブル)の具体的な例を示した図である。この図11に示したように、デジタルコピー制御記述子は、デジタル記録機器におけるコピー世代を制御する情報および最大伝送レートの記述をしたものであり、先頭(図中左側)から8ビットの「記述子タグ」、8ビットの「記述子長」、2ビットの「デジタルコピー制御情報」、1ビットの「最大伝送レートフラグ」、1ビットの「コンポーネント制御フラグ」、2ビットの「コピー制御タイプ」および2ビットの「APSS制御データ」を含んでいる。

【0100】

「記述子タグ」は、デジタルコピー制御記述子の始まりを示すと共に、記述子の識別するためのものである。「記述子長」は、記述子の長さ(領域)を示したものである。

【0101】

「デジタルコピー制御情報」は、デジタルコンテンツの複写(コピー)を制御する情報であり、「コピー不可」「コピー世代」「コピー自由」等に分けられている。「最大伝送レートフラグ」は、最大伝送レートを識別するためのフラグである。

【0102】

「コンポーネント制御フラグ」は、コンポーネント(映像、音声、データ等)毎にコピー制御情報が付与されている場合に1となるもので、この場合、コンポーネント毎にコピー制御情報が記述されている。「APSS制御データ」は、APSS(Audio Processor System)を制御するための情報である。

【0103】

以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。

【0104】

例えば、コンテンツ送信装置1、1A、コンテンツ受信装置21、21Aの各構成の処理を一つずつの過程ととりえたコンテンツ送信方法、コンテンツ受信方法とみなすことや、各構成の処理を汎用のコンピュータ言語で記述したコンテンツ送信プログラム、コンテンツ受信プログラムとみなすこともできる。

【0105】

これらの場合、コンテンツ送信装置1、1A、コンテンツ受信装置21、21Aのそれぞれと同様の効果を得ることができる。また、コンテンツ送信プログラムおよびコンテンツ受信プログラムとした場合には、これらのプログラムを記録媒体等に記録して流通させることもできる。

【0106】

【発明の効果】

請求項1、2、4記載の発明によれば、コンテンツが第一暗号鍵で暗号化され、暗号化コ

10

20

30

40

50

コンテンツとされる。コピー制御情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、暗号化コンテンツ、コピー制御情報および第一暗号鍵関連情報が多重化され送出される。このため、受信側にて、多重暗号化コンテンツに多重化されている関数演算情報と、受信側で送信側の所定関数と同様の所定関数でコピー制御情報が演算されて得られたものとが比較されれば、この比較結果に基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。

【0107】

請求項3記載の発明によれば、コンテンツが第一暗号鍵で暗号化され、暗号化コンテンツとされる。また、コピー制御情報を含む利用条件情報が所定関数で演算され、関数演算情報に加工される。そして、第一暗号鍵および関数演算情報が第二暗号鍵で暗号化され、第一暗号鍵関連情報とされる。その後、暗号化コンテンツ、利用条件情報および第一暗号鍵関連情報が多重化され送出される。このため、受信側にて、多重暗号化コンテンツに多重化されている関数演算情報と、受信側で送信側に備えられる所定関数と同様の所定関数で利用条件情報が演算されて得られたものとが比較され、さらに利用条件情報に基づいて、暗号化コンテンツを復号化可能かが判定されれば、これら比較結果および判定結果に基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。さらに、コンテンツの制作者（放送事業者）の意図に応じて、利用条件情報

10

20

【0108】

請求項5、6、8記載の発明によれば、受信された多重暗号化コンテンツが暗号化コンテンツおよびコピー制御情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。送信側に備えられている所定関数と同様の所定関数で、コピー制御情報が演算され、比較用関数演算情報とされる。関数演算情報と比較用関数演算情報とが比較され、この比較結果に基づき、第一暗号鍵の送出が制御される。その後、暗号化コンテンツが第一暗号鍵で復号化されて出力される。このため、多重暗号化コンテンツに多重化されている関数演算情報と、送信側に備えられる所定関数と同様の所定関数でコピー制御情報が演算されて得られたものとが比較され、この比較結果に基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。

30

【0109】

請求項7記載の発明によれば、受信された多重暗号化コンテンツが暗号化コンテンツと、利用条件情報と、第一暗号鍵関連情報とに分離される。続いて、第一暗号鍵関連情報が第二暗号鍵で復号化され、この第一暗号鍵関連情報に含まれている第一暗号鍵および関数演算情報が取得される。送信側に備えられている所定関数と同様の所定関数で、利用条件情報が演算され、比較用関数演算情報とされる。関数演算情報と比較用関数演算情報とが比較され、暗号化コンテンツが復号化可能かが判定され、これら比較結果、判定結果に基づき、第一暗号鍵の送出が制御される。その後、暗号化コンテンツが第一暗号鍵で復号化されて出力される。このため、多重暗号化コンテンツに多重化されている関数演算情報と、送信側に備えられる所定関数と同様の所定関数で利用条件情報が演算されて得られたものとが比較され、この比較結果と、利用条件情報に基づいて、暗号化コンテンツを復号化可能かが判定され判定結果とに基づいて、コンテンツが利用可能かどうかを判定することができる。これにより、コンテンツの不正コピーの防止、または、不正なコピー制御情報を含むコンテンツの生成を防止することができる。さらに、送信側のコンテンツの制作者（放送事業者）の意図に応じた利用条件情報に基づいたコンテンツの利用（再生）を実現する

40

50

ことができる。

【図面の簡単な説明】

【図 1】本発明による一実施の形態であるコンテンツ送信装置のブロック図である。

【図 2】本発明による一実施の形態であるコンテンツ受信装置のブロック図である。

【図 3】図 1 に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図 4】図 2 に示したコンテンツ受信装置の動作を説明したフローチャートである。

【図 5】図 2 に示したコンテンツ受信装置の動作を説明したフローチャートである（図 4 の続き）。

【図 6】本発明による他の実施の形態であるコンテンツ送信装置のブロック図である。

【図 7】本発明による他の実施の形態であるコンテンツ受信装置のブロック図である。

10

【図 8】図 6 に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図 9】図 7 に示したコンテンツ受信装置の動作を説明したフローチャートである。

【図 10】図 7 に示したコンテンツ受信装置の動作を説明したフローチャートである（図 9 の続き）。

【図 11】デジタルコピー制御記述子の例を説明した図である。

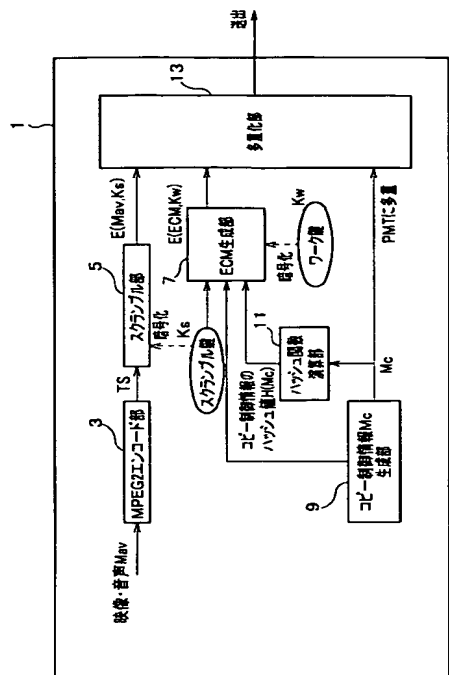
【符号の説明】

1、1 A	コンテンツ送信装置
3	MPEG2 エンコード部
5	スクランブル部
7	ECM 生成部
9	コピー制御情報 MC 生成部
11、27	ハッシュ関数演算部
13	多重化部
21、21 A	コンテンツ受信装置
23	受信分離部
25	コピー制御情報 MC 抽出部
29、29 A	セキュリティモジュール
31	ECM 解析部
33	比較部
35	送出制御部
37	デスクランブル部
39	MPEG2 デコード部
41	コンテンツ蓄積部

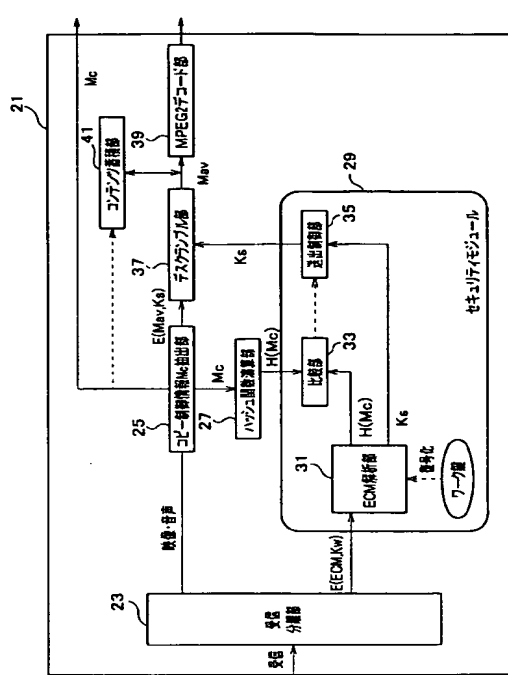
20

30

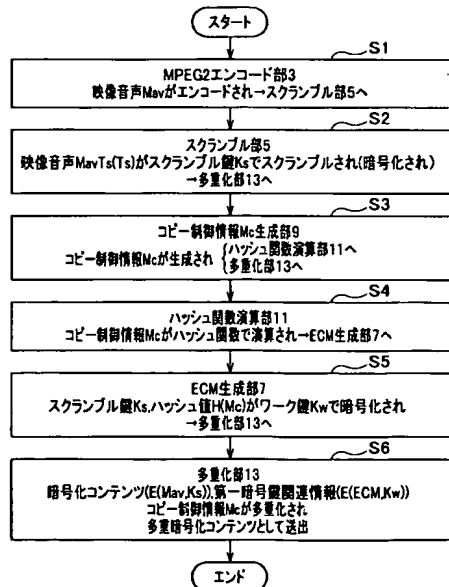
【図1】



【図2】



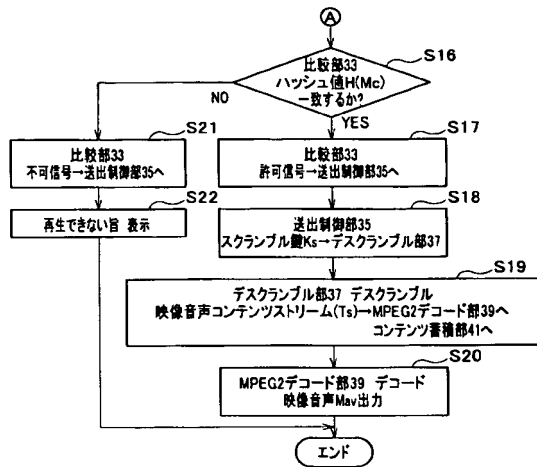
【図3】



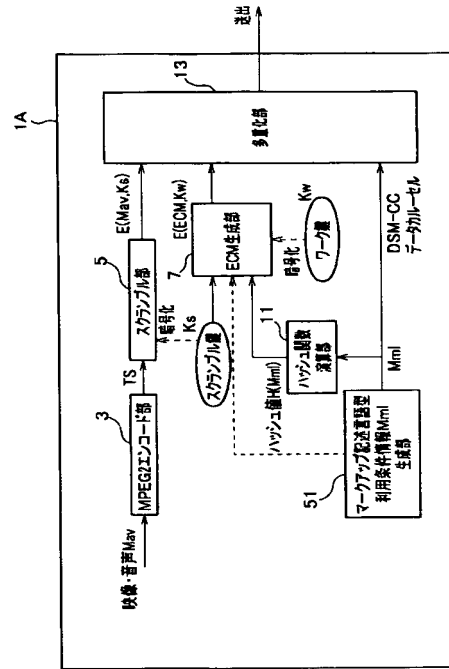
【図4】



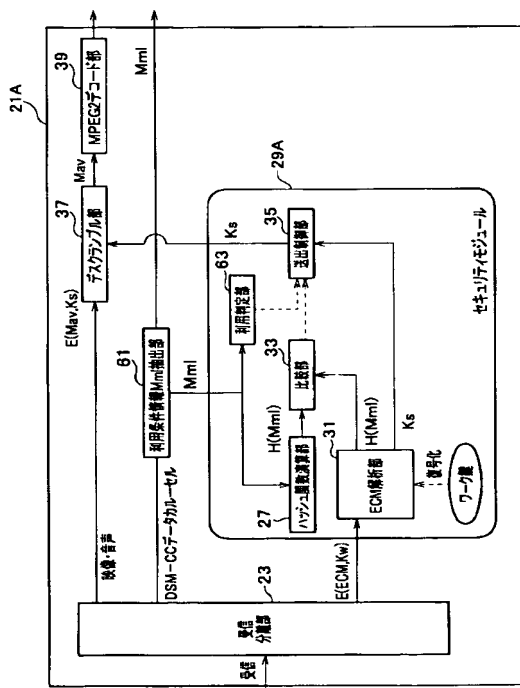
【図5】



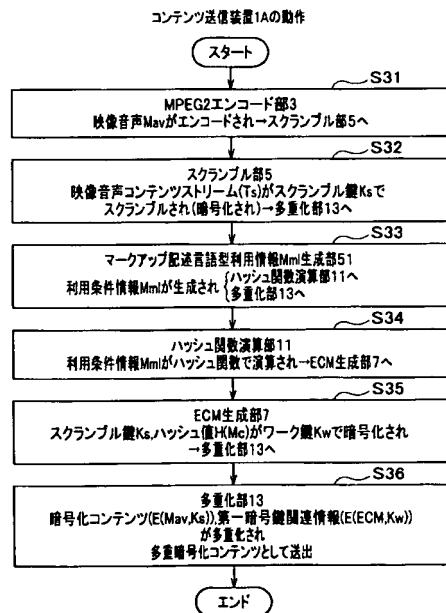
【図6】



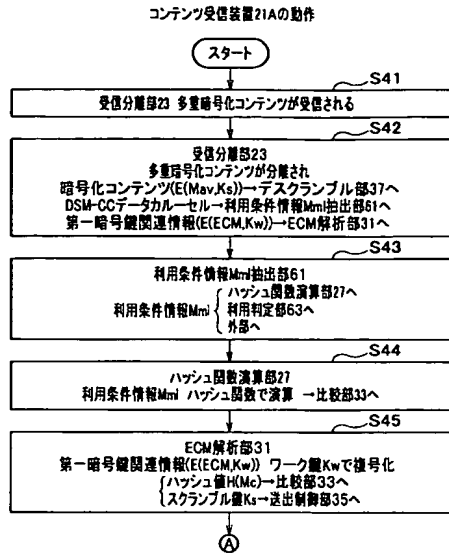
【図7】



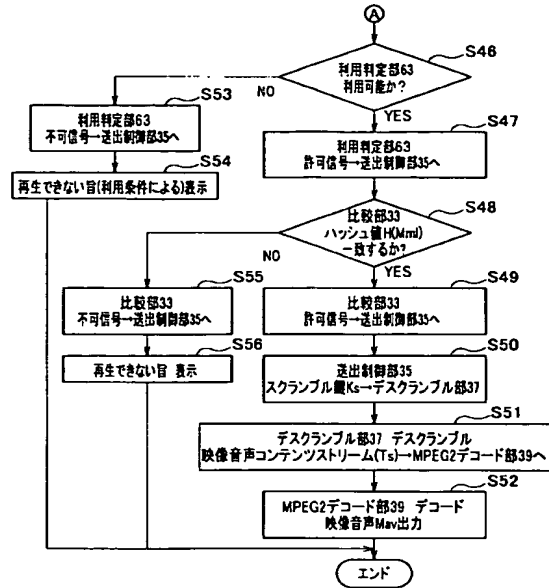
【図8】



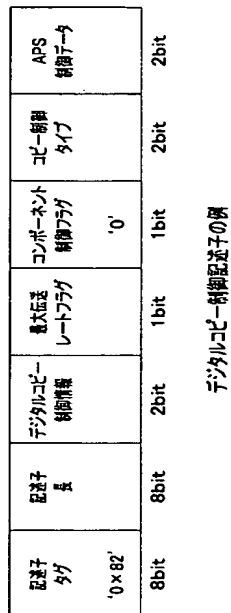
【図 9】



【図 10】



【図 11】



フロントページの続き

(72)発明者 栗岡 辰弥

東京都世田谷区砧一丁目10番11号

日本放送協会 放送技術研究所内

Fターム(参考) 5B017 AA06 BA09 BB10 CA16

5C064 BA01 BB02 BC06 BC17 BC22 BC23 BD02 BD08 BD09 CA14

CB01 CC04

5J104 AA08 AA12 AA16 BA04 EA04 EA15 NA02 NA03 NA12 PA07